IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

GERALD KNOLL, an individual, Plaintiff, vs. ELAINE DOE, JOHN DOE, and JOHN DOES II-XX, Defendants *in personam*, - and - 493.39 ETHER, 1.01 BITCOIN, and 37,195.20 TETHER VIRTUAL CURRENCY, Defendants *in rem*.	Case No.: VERIFIED COMPLAINT Jury Trial Demanded

COMES NOW the Plaintiff, Gerald Knoll, by and through his undersigned counsel Joseph R. Casey of Harding Law Offices and Joseph M. Conboy of Kralovec Conboy, and sets forth his Verified Complaint against Defendant Elaine Doe ("Elaine Doe"); Defendant John Doe ("John Doe"); Defendants John Does II-XX (collectively the "John Doe Defendants"); and *In Rem* Defendants 493.39 Ether ("ETH Defendant"), 1.01 Bitcoin ("BTC Defendant"), and 37,195.20 Tether Virtual Currency ("USDT Defendant"); as follows:

NATURE OF THE ACTION

1. This is a civil action arising under 18 U.S.C. § 1962 et seq. and multiple tortious acts in violation of Illinois statutory and common law.
2. The matter stems from a romance scam. As part of their scheme to defraud Plaintiff, Defendants induced Plaintiff to withdraw his retirement funds, savings, and incur debt in

order to purchase more than $1,200,000.00 in cryptocurrency. The present value of those stolen assets exceeds $2,001,414.95.

3. All of the virtual assets, based on the Bitcoin and Ethereum blockchains, were converted from Plaintiff by Defendants into multiple types of cryptocurrencies– through a process of fraudulent conveyances – and shuffled through a variety of wallets controlled by the Defendants before being deposited at various cryptocurrency exchanges, where the scammers can "cash out" the stolen cryptocurrency.

4. The theft occurred through an increasingly common and sophisticated fraudulent scheme known as a "pig-butchering scam," wherein victims such as Plaintiff are "fattened" for financial slaughter by tricking the victim into a romantic relationship with a scammer hiding behind fraudulent social media profile before eventually deceiving the victim into handing over cryptocurrency to the scammer's website, which is typically designed to mimic a legitimate cryptocurrency exchange.

5. Plaintiff was one victim of this type of "romance scam." Consumer losses in similar scams have been staggering, generating extensive media attention, with some calculations suggesting that consumers worldwide have lost as much as $75 billion to scammers.[1]

6. Defendants took numerous measures to obscure the resulting transaction trail left behind on the Bitcoin and Ethereum blockchains. These transactions are traceable and, have in fact been traced, by Plaintiff.

7. Plaintiff's investigation has led him to initiate recovery actions in the United States, where recovery of the stolen assets may be affected, as Defendants currently possess or control

[1] *See*, for example, Zeke Faux, "Pig-butchering' crypto scams have tricked investors out of more than $75 billion, according to a new study." *Fortune Magazine* (29 February 2024) (available at https://fortune.com/2024/02/29/pig-butchering-crypto-scams-nab-over-75-billion-use-tether-binance-says-study/ as of 2 May 2024).

all or a significant portion of Plaintiff's stolen property or proceeds therefrom through their accounts at the cryptocurrency exchanges operated by Binance Holdings LTD d/b/a Binance.com and Foris DAX, Inc. d/b/a Crypto.com ("crypto.com"). While Binance Holdings LTD operates outside of U.S. jurisdiction, Foris DAX, Inc. is a domestic U.S. corporation serving U.S. residents.

8. Undersigned counsel has been in contact with outside counsel for the Crypto.com exchange who, relying on information from Plaintiff's forensics expert, identified one of their U.S. customers – an Illinois resident listed in this action as John Doe I – as a recipient of Plaintiff's stolen assets. Crypto.com has voluntarily frozen their customer's account during the pendency of this action.

9. Plaintiff's case is particularly unusual because the Defendants have not ceased all communications with Plaintiff (as is the usual practice with pig-butchering scams), as the Defendants do not yet know Plaintiff has determined that he has been scammed or located his stolen assets. This case, therefore, poses unique potential for a rare recovery.

PARTIES, JURISDICTION, AND VENUE

10. Plaintiff Gerald Knoll ("Knoll") is a natural person residing in Albuquerque, Bernalillo County, New Mexico.

11. Defendant Elaine Doe is an individual whose true residence is unknown. Plaintiff believes she is the "lead" scammer with whom Plaintiff has been in contact during the course of the scheme against him, and that Defendant Elaine Doe is a colleague of Defendant John Doe and Defendants John Does II-XX. Plaintiff will attempt to identify Defendant Elaine Doe through discovery served on known third parties with whom Defendants interacted and through additional investigation of the theft and subsequent transfers of the stolen assets.

As of the date of this Complaint, Plaintiff has information and reason to believe Defendant Elaine Doe is a resident of the United States, as she has represented to Plaintiff that she is a Japanese expatriate living in Miami, Florida, although her true domicile is unknown.

12. Defendant John Doe is an individual who, upon information and belief provided by non-party cryptocurrency exchange Crypto.com, resides in Chicago, Illinois. Plaintiff believes Defendant John Doe is a U.S.-based colleague of the remaining *in personam* defendants. Plaintiff will attempt to identify Defendant John Doe through discovery served on known third parties with whom all Defendants interacted and through additional investigation of the theft and subsequent transfers of the stolen assets.

13. John Doe Defendants II-XX are individuals of unknown residence who, upon information and belief, assisted Defendants Elaine Doe and John Does I in perpetuating the wrongdoing alleged herein. Plaintiff will attempt to identify Defendants John Does II-XX through discovery served on known third parties with whom Defendants John Does II-XX interacted and through additional investigation of the theft and subsequent transfers of the stolen assets. As of the date of this Complaint, Plaintiff has information and reason to believed Defendants John Does II-XX are domiciled in the Republic of the Philippines.

14. Defendant *in rem* 493.39 Ether is a cryptocurrency native to the Ethereum network, a decentralized blockchain.

15. Defendant *in rem* 1.01 Bitcoin is a cryptocurrency native to the Bitcoin network, a decentralized blockchain.

16. Defendant *in rem* 37,195.20 Tether Virtual Currency is an ERC-20 cryptocurrency native to the Ethereum blockchain.

17. The Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1331, as Plaintiff's claims include a cause of action pursuant to 18 U.S.C. § 1964(a).

18. The Court also has jurisdiction over this matter pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds $75,000.00, exclusive of interest, costs and attorneys' fees, and is an action between citizens of different states or subjects of foreign states.

19. The Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

20. Jurisdiction and venue are proper in the Northern District of Illinois because the conduct giving rise to this action – including the Defendants' conduct inducing Plaintiff to transfer assets which Defendants used as part of their tortious scheme – occurred at least in part in Chicago, Illinois; and as a result of Defendants' conduct, directed and induced Plaintiff to send digital assets which Defendants deposited at their Crypto.com account; and accessed said funds via computer systems in Chicago, Illinois and, upon information and belief, used Illinois banks to receive proceeds from the scheme.

FACTUAL BACKGROUND

21. Plaintiff hereby incorporates by reference paragraphs 1-20 as if fully set forth herein.

22. On or before 20 September 2023, Plaintiff accepted a Facebook "friend request" from an individual who held herself out as "Elaine Cnao" (hereinafter "Defendant Elaine Doe"). Plaintiff accepted the "friend request." She represented herself as living in Miami but being originally from Japan.

23. On or about 20 September 2023, Defendant Elaine Doe began communicating via Facebook Messenger, an in-app messaging application, and suggested to Plaintiff that he and Defendant Elaine Doe should become acquainted. Defendant Elaine Doe proposed that

she and Plaintiff use the WhatsApp and Telegrams messaging applications for these purposes, and Plaintiff complied. Defendant Elaine Doe's WhatsApp and Telegrams accounts showed a phone number (the sole identifier tied to WhatsApp and Telegram accounts and the sole piece of data needed for establishing an account) of +1 (786) 558-6385.

24. Between 20 September 2023 and 20 April 2024, Defendant Elaine Doe and Plaintiff built a romantic relationship and became friends, messaging each other regularly.

25. On or about 29 September 2023, Defendant Elaine Doe stated to Plaintiff that she had an interest in cryptocurrency and that she was a successful amateur trader of cryptocurrency-based options contract. She further represented that her success was due to information leaked by her godmother, whom Defendant Ellie Doe portrayed as a well-connected former bank employee with valuable insights into Bitcoin options trading. This information piqued Plaintiff's interest, despite having no personal experience in purchasing, owning, or trading cryptocurrency.

26. On or about 29 September 2023, Defendant Elaine Doe offered to teach Plaintiff how to purchase options contracts with the goal of making profits which would help Plaintiff reach his personal financial goals.

27. On or about 29 September 2023, at Defendant Elaine Doe's direction and inducement, Plaintiff opened an account at Coinbase.com, a U.S. cryptocurrency exchange.

28. Between 29 September 2023 and 20 April 2024, at Defendant Elaine Doe's direction and inducement, Plaintiff made several large, interstate wire transfers of U.S. dollars from his checking account in New Mexico to his account at Coinbase.com via Coinbase's intermediary bank. In all, at Defendant Elaine Doe's direction, Plaintiff liquidated and sent

to the Defendants more than $1,200,00.00 worth of cryptocurrency, derived from a home refinancing, his life savings, and retirement accounts.

29. At the direction and inducement of Defendant Elaine Doe, Plaintiff exchanged his U.S. Dollars into three cryptocurrencies:

    a. Ether, a cryptocurrency native to the Ethereum blockchain and abbreviated on cryptocurrency exchanges as "ETH." ETH is created and maintained by the decentralized Ethereum network.

    b. Bitcoin, the cryptocurrency native to the Bitcoin blockchain and abbreviated on cryptocurrency exchanges as "BTC." BTC is created and maintained by the decentralized Bitcoin network.

    c. Tether, a cryptocurrency native to the Ethereum blockchain and abbreviated on cryptocurrency exchanges as "USDT" (U.S. Dollar Tether). Tether is created and maintained by Tether Operations Limited, a corporation domiciled in the British Virgin Islands.

30. ETH, BTC, and USDT, like many cryptocurrencies, are a type of highly divisible, fungible token (electronic coin or digital asset) that exists on a blockchain as a digital medium of exchange. While ETH and BTC tokens derive their value from the price which other users/holders of those tokens will pay to purchase those tokens, USDT is "tethered" or pegged to the value of the U.S. Dollar.

31. Defendant Elaine Doe assisted Plaintiff in executing his own options contracts or cryptocurrency trades on a purported cryptocurrency exchange called Zaifint (also branded Zaif, ZAIF or Zaif INT), which uses the domain "zaifint.com."[2] The website's name is

[2] Undersigned counsel, Mr. Casey, is currently litigating another victim of this same scam involving the fake Zaif.com website, with likely different individual *in personam* defendants. The plaintiff in that matter is still attempting to

similar to a legitimate cryptocurrency exchange website – "zaif.jp" – based in Japan. The scam is still ongoing as of the date of this filing, now using www.zaifint.org.

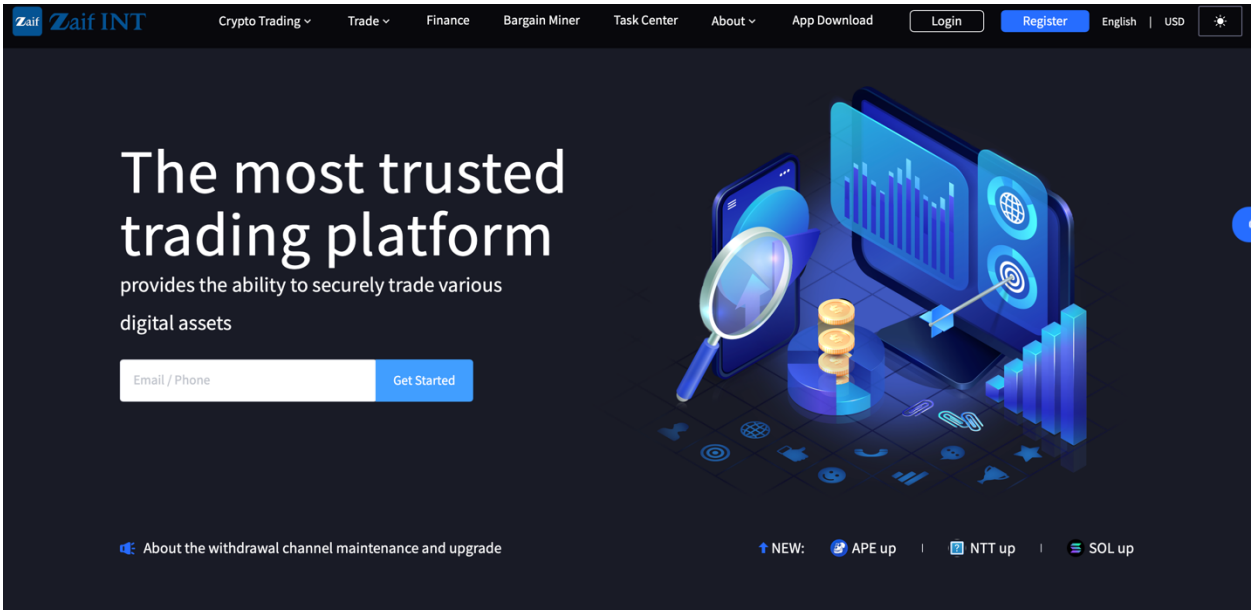

Figure 1 -
A screenshot of the home page for the Zaifint fake exchange interface

32. The Zaifint interface was also available on application stores for download to iPhone and Android. Its listed publisher is "Ardaa Eskici," which, upon information and belief, is a pseudonym used by the John Doe defendants.

discover the true identities of the persons or entities behind the scam website, and notes that some of the information discovered in that action is subject to protective orders. The matter is *Bullock v. Doe et al.*, Case No. 3:23-cv-03041-CJW-KEM (N.D. Iowa).

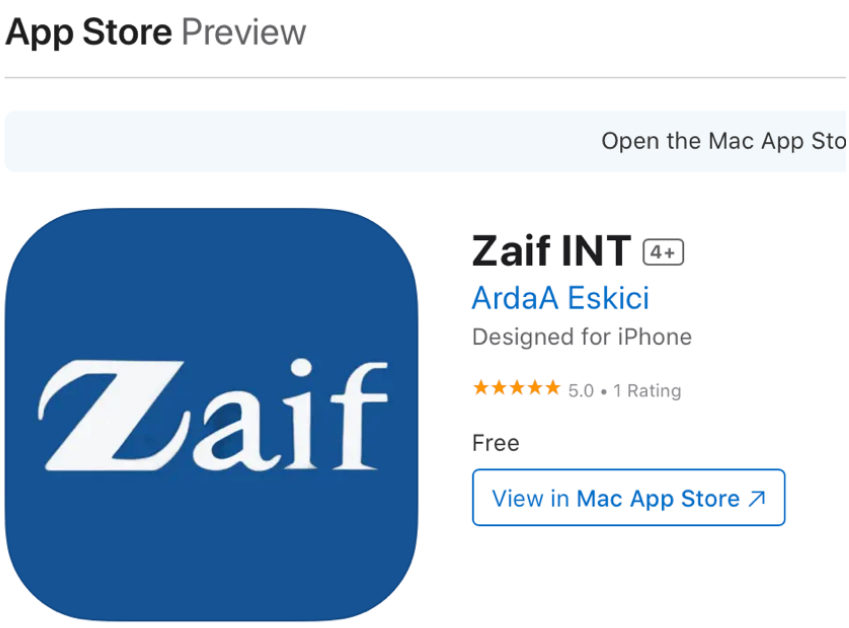

Figure 2 –
A screenshot of Zaifint as it appears on Apple's App Store

33. Throughout the course of the scam against Plaintiff, Defendant Elaine Doe provided step-by-step instructions for Plaintiff to execute each trade by performing transactions on the Ethereum blockchain.

34. Each transaction Plaintiff completed involved sending certain amounts of ETH, BTC, and USDT to several destinations, namely cryptocurrency wallets (designated by their blockchain addresses, a unique string of letters and numbers commonly known as "addresses") capable of receiving cryptocurrency on the Ethereum and Bitcoin blockchains.

35. Defendant Elaine Doe provided these addresses to Plaintiff and represented that the addresses belonged to the Zaifint platform when, in reality, the addresses were controlled by her, John Doe I, and John Does II-XX.

36. To induce large deposits from Plaintiff, Defendant Elaine Doe represented to Plaintiff that she had deposited a sum certain worth of cryptocurrency into a Zaifint account on his behalf, which he could repay after a period of successful trading and withdrawal from the platform.

37. Defendant Elaine Doe then provided step-by-step instructions and supervised Plaintiff in making thirty-six (36) transactions from 30 September 2023 to 25 March 2024, sending specific amounts of ETH, BTC, and USDT from Plaintiff's account at Coinbase to the purported Zaifint addresses.

38. After Plaintiff completed each transaction, by manipulating the website with the help of the remaining Defendants, Defendant Elaine Doe showed Plaintiff a display on Zaifint which purported to reflect that Plaintiff earned a sizeable profit on each trade.

39. In reality, the ETH, BTC, and USDT Plaintiff sent to "Zaifint" went directly into addresses controlled by Defendant Elaine Doe and/or the remaining Defendants. Zaifint did not and does not exist as a legitimate website, investment platform, or cryptocurrency exchange.

40. Plaintiff lacked the technological sophistication to verify the owner of the addresses to which he was sending ETH, BTC, USDT, learn about the operator of Zaifint, or detect that Zaifint was neither a real website nor a legitimate cryptocurrency exchange.

41. By April 2024, Plaintiff believed his "trades" on Zaifint had grown and earned him a substantial profit.

42. As early as 1 December 2023, Defendant Elaine Doe had assisted Plaintiff in contacting the remaining Defendants – persons she alleged were employees at the fake Zaifint exchange through Zaifint's account Telegram, an instant messaging service. Together with the remaining Defendants, Defendant Elaine Doe helped Plaintiff deposit, manage, and

eventually seek the return of Plaintiff's crypto to his Coinbase account. Zaifint.com's website and Defendant Elaine Doe directed Plaintiff to the same Telegram account.

43. Through Zaifint's Telegram account, a purported representative (or team of representatives) from Zaifint conveyed an extortionary threat to Plaintiff, represented to Plaintiff that it would not release his funds until he submitted to Zaifint confidential, personally-identifying and financial information. They also required he make an additional transfer of 10% of the value of crypto he believed he had deposited and earned with Zaifint, or approximately $700,000.00

44. When Plaintiff attempted to withdraw at least $300,000.00 in digital assets or their U.S. dollar equivalent, the Zaifint representative(s) told Plaintiff that his account had been frozen, his funds seized or otherwise inaccessible, and threatened to harm his consumer credit rating. Zaifint and all Defendants have since refused to return Plaintiff's funds.

45. After these interactions, Plaintiff has discovered that Defendant Elaine Doe and the Zaifint representatives had perpetrated against him a new and sophisticated version of an online scheme known as a "pig-butchering scam" according to the following model:

    a. One or more cybercriminals hiding behind entirely fabricate online personas (a "lead" scammer) form an extended, emotional relationship with their intended victim over an instant messaging application;

    b. After months of building trust with their victim (or "pig"), the lead scammer introduces the victim to the concept of generating income through trading cryptocurrency and guiding the victim through steps required to send money to the scammer's cryptocurrency addresses;

c. Relying on their victim's emotional dependence and lack of technical sophistication, the scammer shows their victim a website designed to look like a legitimate cryptocurrency exchange, but whose domain, interface, and features they control;

d. The scammer then uses this website to excite the victim with legitimate-looking charts and diagrams which reflect the victim's purported trades and profits;

e. In reality, each transaction in which the victim believes they are sending cryptocurrency to an exchange goes directly into the scammer's private addresses, after which the scammer performs a rapid series of transfers between other addresses controlled by the scammer in an attempt to disguise the final address holding the stolen cryptocurrency before distribution to the scammers (named here as the co-defendants);

f. Once the scammer has convinced the victim that their financial goals have been made possible by the fake exchange, the scammer "butchers" their victim by demanding (through the exchange's chat function) one final payment. The lead scammer may even threaten the victim in an attempt to coerce further payment; and

g. Whether or not the victim makes an additional payment, the scammers keep all of the victim's funds and vanishes from the instant messaging platform used to communicate with the victim.

46. Upon information and belief, Defendants John Doe and John Does II-XX participated in this scheme to defraud Plaintiff by:

a. assisting Defendant Elaine Doe by participating in communication with Plaintiff under the name "Elaine" or "Ellie" and facilitating her scheme against him;

b. providing images which they represented showed Defendant Elaine Doe;

c. operating the cryptocurrency addresses used in the scam and the wallets containing those addresses;

d. operating and funding the telephone number used in the scam;

e. operating a Facebook account used to perpetuate the scam;

f. operating the WhatsApp account used to perpetuate the scam;

g. operating a Telegram account used to perpetuate the scam;

h. building, funding, and operating a website for the fake cryptocurrency exchange website known as Zaifint.com;

i. building, funding, deploying, and operating a mobile iOS and Android application for the fake cryptocurrency exchange website known as Zaifint.com;

j. falsely posing as customer service representatives for a cryptocurrency exchange;

k. transferring those funds to Binance.US and Crypto.com exchange accounts and swapping them for US Dollars or other fiat currencies; and

l. otherwise engaging in tortious and illegal conduct against Plaintiff.

47. All Defendants engaged in the scheme set forth above. Through expert forensic testimony and exposition of public blockchain records, Plaintiff will prove that Defendants stole Plaintiff's assets and then shuffled them through "shell" blockchain addresses used by the Defendants to deprive Plaintiff of his digital assets and conceal their identities and the destination of the stolen assets. For example, in the last example of Plaintiff being defrauded into sending cryptocurrency to Defendants, the forensic pathway for the theft and subsequent transactions follows this path:

a. On 25 Mar 2024 Plaintiff sent 5.21808331 ETH from his Coinbase account to 0xa97b6e171c0ac20E4914855572B00F7D3F00153b (Scam Address 7).

b. On 25 Mar 2024 at 08:28:47 PM +UTC Defendants sent 5.216430557437546 ETH ($20,058.50) from Scam Address 7 to 0xF186878447A03aff041148dC46b7640E67cDB287 in TX 0xa17adc7ab85856049ce18fb4fb6b88110641044747d64a9c40ff68662a3b996f.

c. On 25 Mar 2024 at 09:23:35 PM +UTC Defendants sent 5.215596533429092 ETH from 0xF186878447A03aff041148dC46b7640E67cDB287 to 0x31Ab1eb2c50F567Bf8F237dfEfB2Ea5A43dd98e3 in 0x436a2d50fb9d69b140681ae30b5f100ce3484b3ada014d185b9854e8a146dbe5.

d. After commingling with other tokens, on 27 Mar 2024 at 01:39:23 AM +UTC, Defendants used Tokenlon via 0x31Ab1eb2c50F567Bf8F237dfEfB2Ea5A43dd98e3 to convert the assets to WETH, then swapped for $28,924.29 USDT on 0X protocol in TX 0x64df528d1d6b1168df1d4bb25e4a3013386cbefcd58dd0c5d7583f9105d88116. This resulted in a deposit of 28,854.880138 USDT at 0x31Ab1eb2c50F567Bf8F237dfEfB2Ea5A43dd98e3.

e. On 28 Mar 2024, 03:40:11 PM +UTC Defendants via 0x31Ab1eb2c50F567Bf8F237dfEfB2Ea5A43dd98e3 sent 33,500 USDT to 0xFb6b667b7017CAc942dD8026f37C94293c5Dfa77 in TX 0xf6a51abfd44b41eb0a7aefbc4ba8e81d72088481c62c7ffbb9daa935c2a20d1e.

f. On 28 Mar 2024, 03:41:59 PM +UTC Defendants sent 33,165 USDT from 0xFb6b667b7017CAc942dD8026f37C94293c5Dfa77 to

0xA2cd7f7f48650B83789E7ba0797Fec15aF3Ff5a0 in TX 0x726e641e9320b196cdf1ba2d2b0a80e8aa11270ba88968e77a697c61610c99bd.

g. On 28 Mar 2024 at 04:43:11 PM +UTC Defendants sent 33,165 USDT from 0xA2cd7f7f48650B83789E7ba0797Fec15aF3Ff5a0 to Crypto.com Hot Wallet (0xf3b) 0xf3B0073E3a7F747C7A38B36B805247B222C302A3.

48. In all, Defendants used seven (7) principal ETH, BTC, and USDT addresses to receive Plaintiff's crypto before shuffling it through dozens of addresses. Plaintiff incorporates by reference **Exhibit A**, which sets forth the affidavit of Plaintiff's Expert Witness attesting to the general allegations of this Complaint and the specific transactions set forth in ¶ 47.

49. To this day, Defendants wrongfully possess Plaintiff's assets or their fiat currency equivalent in one or more crypto wallets and accounts controlled by Defendants at Binance and Crypto.com, including John Doe II, the believed owner of the frozen Crypto.com account:

a. Binance 14: 0x28C6c06298d514Db089934071355E5743bf21d60

b. Crypto.com: 0xf3B0073E3a7F747C7A38B36B805247B222C302A3

50. All of these addresses used to steal from Plaintiff in direct transfers from Coinbase.com (hereinafter "Scam Addresses") are and were directly or indirectly controlled by Defendants Elaine Doe, John Doe, and John Does II-XX, just as the subsequent transfer addresses are and were under their control:

a. The addresses used to convert funds ("Scam Addresses") are as follows:

ADDRESS SHORTHAND	ETHEREUM AND BITCOIN ADDRESSES
Scam Primary Address 1	16p6Spz76kTpmzBpvsvL3pAeqEmz18SR4a
Scam Primary Address 2	3QHvf3J7zizfaXVUHq73sRRLsfbTNuPNQh
Scam Primary Address 3	0xc3891763dE0043a241b46e585fd3ea326730D004
Scam Primary Address 4	0x67c16C4BE3D66D4727562968D0A67f89DD5267A6
Scam Primary Address 5	0xe04fBB92F6AC735471a82Bb174382D919CDa375a
Scam Primary Address 6	19jGBh1co3aguxvwEtUPqv7BZtCbLsTkY9

Scam Primary Address 7	0xa97b6e171c0ac20E4914855572B00F7D3F00153b

b. Of the above-referenced addresses, Defendants used seven (7) Scam Addresses) as "primary wallets," meaning that they were the first addresses used to receive the Plaintiff's stolen funds in a transaction with Plaintiff.

c. Of the above-referenced addresses, Defendants used dozens of Scam Addresses as "sub-addresses," meaning that they were not the first addresses used to receive Plaintiff's stolen crypto in a transaction with Plaintiff but were instead transactions from one address controlled by the Defendants to another address used by the Defendants.

d. The Defendants used sub-addresses to fraudulently transfer funds between multiple shell addresses controlled by Defendants and, ultimately, to the Defendants' Binance and Crypto.com exchange account(s) and conceal the theft and destination of funds.

e. The stolen crypto controlled by Defendants' accounts at Binance and Crypto,com are currently in the form of ETH, BTC, and USDT which the Defendants obtained by swapping Defendants' stolen crypto on the Ethereum and Bitcoin blockchain, including by interacting with a fraudulent smart contract and Tokenlon, a decentralized exchange.

51. Aside from the objective and permanent record available on the Ethereum and Bitcoin blockchains (which proves the transactions in question), Plaintiff's evidence – documenting the Defendants' conduct, electronic communications, intent to defraud using electronic wires and bank transfers – consists of many screenshots and preserved conversation transcripts.

52. Defendants do not yet know that Plaintiff has uncovered their scheme, located the stolen assets, and identified exchanges used by Defendants.

FIRST CAUSE OF ACTION
CONVERSION
(Defendants Elaine Doe, John Doe, and John Does II-XX)

53. Plaintiff hereby incorporates by reference paragraphs 1-52 of this Complaint as though fully set forth herein.

54. On or about 1 December 2023, Defendants refused to return Plaintiff's funds when, posing as customer service representatives for the fake exchange known as Zaifint, they told Plaintiff his funds would only be released if he paid additional funds directly to Defendants.

55. Plaintiff owns and has a possessory right to his cryptocurrency retained by Defendants.

56. Defendants have no rightful ownership or possessory interest in Plaintiff's cryptocurrency.

57. Defendants wrongfully maintain possession and dominion over Plaintiff's cryptocurrency.

58. Defendants' possession of Plaintiff's cryptocurrency and wrongfully deprives Plaintiff of the benefits of his property.

59. Defendants' possession of Plaintiff's cryptocurrency is inconsistent with, and in derogation of, Plaintiff's ownership and possessory rights.

60. Defendants' possession of Plaintiff's cryptocurrency is in willful and wanton disregard for the rights of Plaintiff. Defendants lack any good faith claim to Plaintiff's funds.

61. Through its continued possession, Defendants have converted Plaintiff's property.

62. As a result of Defendants' tortious conduct, Plaintiff has suffered damages and continues to suffer damages.

SECOND CAUSE OF ACTION
RACKETEERING
18 U.S.C. § 1962(C)
(Defendants Elaine Doe, John Doe, and John Does II-XX)

63. Plaintiff hereby incorporates by reference paragraphs 1-52 and of 54-62 of this Complaint as though fully set forth herein.

64. Defendants Elaine Doe, John Doe, and John Does II-XX are a group of individuals that were and are engaged in interstate commerce and are associated in fact for the common and shared purpose of (1) profiting by exchanging cryptocurrency assets on cryptocurrency exchanges, while also engaged in criminal acts; (2) operating a fraudulent enterprise designed to steal digital assets from Plaintiff after convincing him to send those digital assets to a fake cryptocurrency exchange controlled by Defendants; (3) funneling those funds into a series of Ethereum and Bitcoin addresses to hide the origin and destination of those stolen assets; (4) then using those stolen assets in otherwise legitimate cryptocurrency trading; (5) maintaining their activities and enterprise through a series of specific threats of financial or reputational harm, leaving victims in an ongoing state of fear for the safety of their person, reputation, identity and financial condition.

65. Defendants Elaine Doe, John Doe, and John Does II-XX operated (and continue to operate) the enterprise together.

66. Defendants Elaine Doe, John Doe, and John Does II-XX each participated in the operation and management of the enterprise with the goal of accomplishing the same common and shared purpose.

67. Ethereum and Blockchain ledger transaction records from Defendants Elaine Doe, John Doe, and John Does II-XX reveal that Plaintiff was far from the first victim of their scheme. The Scam Addresses continue to show the proceeds of this relentless enterprise stealing crypto from other victims.

68. As alleged in detail through this Complaint, Defendants Elaine Doe, John Doe, and John Does II-XX, intentionally and knowingly engaged in a pattern of racketeering activity that included transmissions by means of wire, radio, or television communication with intent to defraud.

69. As alleged in detail through this Complaint and its exhibits, Defendants Elaine Doe, John Doe, and John Does II-XX, knowingly and intentionally engaged in a pattern of racketeering activity that included in engaging in monetary transactions in property derived from specified criminally obtained property and unlawful activity.

70. As alleged in detail through this Complaint and its exhibits, Defendants Elaine Doe, John Doe, and John Does II-XX knowingly and intentionally engaged in a pattern of racketeering activity that included conducting financial transactions with the intent to promote the carrying-on of specified unlawful activity and/or to conceal or disguise the nature, location, source, ownership, and proceeds of specified unlawful activity.

71. As alleged in detail through this Complaint and its exhibits, Defendants Elaine Doe, John Doe, and John Does II-XX knowingly and intentionally engaged in a pattern of racketeering activity that included engaging in monetary transactions in property derived from specified unlawful activity and investing racketeering income by using the stolen assets on a cryptocurrency exchange, trading those assets to obtain a profitable return, and obstruction of justice.

72. Defendants Elaine Doe, John Doe, and John Does II-XX, by their conduct and specific written communications, threaten continued unlawful activity into the future with similar purposes, results, participants, victims, and methods of commission.

73. Other individuals – believed to be part of the same scheme recited herein and its perpetrators (Defendants Elaine Doe, John Doe, and John Does II-XX) – have continued to contact and attempt to contact Plaintiff to further defraud him. Plaintiff expects their efforts to persist.

74. The predicate acts of Defendants Elaine Doe, John Doe, and John Does II-XX are not isolated events, and are part of a widespread scheme to defraud other unsuspecting victims (some of whom have sued in U.S. courts) for the same or similar purposes and to achieve the same or similar results through the same or similar methods.

75. Defendants Elaine Doe, John Doe, and John Does II-XX each had their own roles in the enterprise and maintained those roles throughout the course of the scheme, and each personally conducted the affairs of the enterprise.

76. As a foreseeable and natural consequence of the enterprise, Plaintiff has lost more than $2,001,414.95 worth of digital assets.

77. Plaintiff suffered other damages to his property as a result of the fraudulent scheme.

78. Pursuant to 18 U.S.C. § 1964(c), Plaintiff is entitled to an award of three times the actual damages sustained plus the costs of this action and reasonable attorney fees.

THIRD CAUSE OF ACTION
CONSPIRACY TO COMMIT RACKETEERING
18 U.S.C. § 1962(d)
(Defendants Elaine Doe, John Doe, and John Does II-XX)

79. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62 and 64-78 of this Complaint as though fully set forth herein.

80. Even if they did not direct or manage the affairs of the enterprise (which they did), Defendants Elaine Doe, John Doe, and John Does II-XX agreed that someone would commit predicate acts as detailed above.

81. Defendants Elaine Doe, John Doe, and John Does II-XX were each aware of the essential nature and scope of the enterprise, and they intended to participate in it and share its profits.

82. Plaintiff was deprived of money or property that he otherwise would not have lost but for the conduct of the Defendants.

83. As a direct and proximate cause of Defendants Elaine Doe, John Doe, and John Does II-XX's racketeering activities, Plaintiff has been injured through the theft of his digital assets.

84. As a foreseeable and natural consequence of the fraudulent scheme described above, Plaintiff lost more than $2,001,414.95 worth of digital assets.

85. Plaintiff suffered other damages as a result of the fraudulent scheme.

86. Pursuant to 18 U.S.C § 1964(c), Plaintiff is entitled to an award of three times the actual damages sustained plus the costs of this action and reasonable attorneys' fees.

FOURTH CAUSE OF ACTION
NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS
(Defendants Elaine Doe, John Doe, and John Does II-XX)

87. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62 64-78, and 80-86 of this Complaint as though fully set forth herein.

88. As set forth above, Defendants Elaine Doe, John Doe, and John Does II-XX acted negligently and tortiously with respect to Plaintiff.

89. As set forth above, Defendants invaded property and privacy interests of Plaintiff that were protected by statutory and common law.

90. As a result of Defendants' conduct, Plaintiff has suffered emotional distress damages have arising naturally from those invasions of his protected interests.

91. As a direct and proximate result of the conduct of Defendants Elaine Doe, John Doe, and John Does II-XX, Plaintiff has suffered and will continue to suffer mental, emotional, and psychological injuries, including severe emotional distress.

92. Defendants Elaine Doe, John Doe, and John Does II-XX engaged in behavior towards Plaintiff that a reasonable person in their position would know or should have known would inflict or cause emotional distress to Plaintiff.

FIFTH CAUSE OF ACTION
FRAUDULENT MISREPRESENTATION
(Defendants Elaine Doe, John Doe, and John Does II-XX)

93. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62, 64-78, 80-86, and 88-92 of this Complaint as though fully set forth herein.

94. As set forth herein, Defendant Elaine Doe represented to Plaintiff that she was an experienced options trader.

95. As set forth herein, Defendant Elaine Doe represented that Zaifint was an independent website and legitimate cryptocurrency exchange where Plaintiff could safely invest funds, and that she had had substantial financial success performing the trades she would instruct Plaintiff to execute. She omitted the fact that she and/or the remaining defendants controlled Zaifint.

96. As set forth herein, Defendants Elaine Doe, John Doe, and/or John Does II-XX represented to Plaintiff that they were members of a customer service team for a purportedly legitimate website and cryptocurrency exchange, "Zaifint.com."

97. The Defendants' foregoing statements were false and they knew that they were false.

98. Defendants' foregoing representations were material, and Plaintiff would not have lost his funds if not for the Defendants' deceit.

99. Defendants knew their conduct was wrongful and intentionally acted despite this knowledge, or made such representations in reckless disregard of whether the representations were false.

100. Defendants engaged in the above-recited conduct in order to intentionally deceive Plaintiff into sending them his assets, and made the above representations with the intent that Plaintiff would rely on them.

101. Defendants acted out of spite, malice or ill will towards Plaintiff.

102. As an unsophisticated party without experience in blockchain technology or investing, and as a person who genuinely believed he was in a trusting and loving relationship with Defendant Elaine Doe, Plaintiff's reliance on Defendants' representations was justifiable.

103. Defendants' conduct was and is a direct and proximate cause of Plaintiff's losses and damages.

SIXTH CAUSE OF ACTION
VOIDABLE TRANSACTIONS
Illinois Uniform Fraudulent Transfer Act (Ill. 740 ILCS 160)
(Defendants Elaine Doe, John Doe, and John Does II-XX)

104. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62, 64-78, 80-86, 88-92, and 94-103 of this Complaint as though fully set forth herein.

105. Each time Plaintiff sent cryptocurrency to Defendants via the transactions described above, Defendants initiated a rapid series of subsequent transactions (hereinafter "subsequent conveyances") using multiple addresses on the Ethereum and Bitcoin blockchains. The scam addresses and sub-addresses involved in the scheme and the fraudulent transfers are explained throughout this Complaint.

106. These subsequent conveyances essentially created a "shell game" in which the stolen cryptocurrency passes quickly from one address under Defendants' control to another, typically with only momentary delay between transactions, before being shuffled into an address associated with a legitimate cryptocurrency exchange.

107. After Plaintiff's assets passed through each of the shell transactions described above, it finally settled in two addresses controlled by the Defendants' accounts at Binance and Crypto.com

108. Plaintiff's stolen cryptocurrency is traceable to these ultimate addresses.

109. At the moment Defendants made the subsequent conveyances, Plaintiff had legal and equitable claims to the cryptocurrency transmitted thereby.

110. Defendants made the subsequent conveyances in a deliberate effort to disguise the ultimate destination of the stolen cryptocurrency from technologically unsophisticated parties; to avoid its obligations to Plaintiff; to hinder, delay or defraud Plaintiff's efforts to assert his legal and equitable claims; and add a façade of legitimacy to any legitimate cryptocurrency exchange with which the Defendants might interact.

111. Defendants' conduct has no good faith defense and was done deliberately and is a proximate cause of Plaintiff's damages.

112. Plaintiff has incurred damages and continues to incur damages today.

SEVENTH CAUSE OF ACTION
AIDING AND ABETTING TORTIOUS CONDUCT
(Defendants Elaine Doe, John Doe, and John Does II-XX)

113. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62, 64-78, 80-86, 88-92, 94-103, and 105-112 of this Complaint as though fully set forth herein.

114. Each of the Defendants committed the tort of conversion and other unlawful acts (collectively, "the tortious conduct" as described throughout this Complaint), thereby causing financial and emotional injury to Plaintiff.

115. Each of the Defendants knew that their fellow Defendants were going to, and in fact did, engage in the tortious conduct against Plaintiff.

116. Each of the Defendants substantially encouraged and/or substantially assisted Defendant Elaine Doe in committing the tortious conduct.

117. A causal relationship exists between the assistance and/or encouragement of Defendants John Doe and John Does II-XX and the tortious conduct of Defendant Elaine Doe.

118. Defendants John Doe and John Doe II-XX personally profited and enriched themselves at the expense of Plaintiff and his assets because of the conduct of Defendant Elaine Doe.

119. The actions of Defendants Elaine Doe and the remaining Defendants were intentional and wrongful conduct motivated by spite or ill will.

120. The actions of the Defendants were: (a) intentional; (b) done to serve their own interests, having reason to know and consciously disregard the substantial risk that their conduct might significantly injure the rights of others, including Plaintiff as a creditor; or (c) a conscious pursuit of conduct knowing that it created a substantial risk of significant harm to Plaintiff.

121. Defendants, then, should be held jointly and severally liable.

EIGHTH CAUSE OF ACTION
DECLARATORY ACTION
(Defendants 493.39 Ether, 1.01 Bitcoin, and 37,195.20 Tether Virtual Currency)

122. Plaintiff hereby incorporates by reference paragraphs 1-52, 54-62, 64-78, 80-86, 88-92, 94-103, 105-112, and 114-121 of this Complaint as though fully set forth herein.

123. There is an actual and justiciable controversy between Plaintiff and Defendants, concerning the party entitled to enforce the rights of redemption represented by the ETH. BTC, and USDT Defendants.

124. As set forth above, Plaintiff is entitled to the rights of redemption represented by the ETH, BTC, and USDT Defendants because Defendants obtained the ETH, BTC, and USDT Defendants through unlawful and tortious means.

125. Plaintiff is, therefore, entitled to judgment declaring that Plaintiff is entitled to enforce the right of payment represented by the ETH, BTC, and USDT Defendants.

126. A declaratory judgment will serve the useful purpose of clarifying and settling the legal rights of the parties with respect to the rights of redemption and other rights represented by the ETH, BTC, and USDT Defendants. In particular, a declaratory judgment will provide essential clarity to Plaintiff in ascertaining its enforcement options in the event that it obtains a judgment against Defendants.

127. The substantial controversy between the parties having adverse interests is of sufficient immediacy and reality to warrant the issuance of a declaratory judgment, as it is an important and effective remedy available to the parties.

128. By reason of the foregoing, Plaintiff is entitled to judgment declaring that Plaintiff is entitled to enforce the right of payment represented by the ETH, BTC, and USDT Defendants.

NINTH CAUSE OF ACTION
CONSTRUCTIVE TRUST
(Defendants 493.39 Ether, 1.01 Bitcoin, and 37,195.20 Tether Virtual Currency)

129. Plaintiff hereby incorporates by reference paragraphs 11-52, 54-62, 64-78, 80-86, 88-92, 94-103, 105-112, 114-121, and 123-128 of this Complaint as though fully set forth herein.

130. Illinois law provides that an individual with an equitable claim to property that has been the subject of a fraudulent transfer may levy execution on the asset transferred or its proceeds, including through a constructive trust. *Chas. Hester Ent. v. Ill. Founders Ins. Co.*, 114 Ill. 2d 278, 293 (Ill. 1986) ("Where property has been acquired wrongfully, the party in possession may be declared to be a constructive trustee of the property if it would be unjust for that party to retain it."). Such trusts may also be granted when the property has been obtained through duress, coercion or mistake. *Id.* at 293 (citation omitted).

131. Plaintiff has a claim on the ETH, BTC, and USDT Defendants because they constitute the crypto assets (or the proceeds thereof) which were wrongfully and unlawfully taken from Plaintiff and retained by Defendants.

132. Defendants forfeited their rights to the ETH, BTC, and USDT Defendants by engaging in unlawful conduct.

133. In principles of equity and good conscience, the rights of redemption represented by the ETH, BTC, and USDT Defendants should be held in trust by a court-appointed trustee for the benefit of Plaintiff.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

(a) Holding Defendants liable, jointly and severally, for their conduct;

(b) An award of actual damages, in amount no less than $2,001,414.95;

(c) An award of treble damages as permitted or required by law, in an amount no less than $6,004,244.85;

(d) An award of punitive damages in an amount no less than four times Plaintiff's actual losses, or $8,005,659.80;

(e) An award of restitution for Defendants' wrongful conduct;

(f) An award of reasonable attorneys' fees and costs;

(g) An award of interest;

(h) A judgment and award:

a. declaring void as a matter of law the subsequent transactions identified herein and in exhibits hereto; and

i. against Defendants 493.39 Ether, 1.01 Bitcoin, and 37,195.20 Tether Virtual Currency, directing the *in personam* Defendants to transfer to Plaintiff assets substantially equivalent to the value of the stolen crypto assets, including equivalent fiat currency;

ii. declaring that Plaintiff is entitled to enforce the rights of redemption represented by the ETH, BTC, and USDT Defendants;

(i) The creation of a constructive trust;

(j) Such other and further relief that the Court deems reasonable and just.

JURY TRIAL DEMAND

Plaintiff demands trial by jury for all issues so triable.

Respectfully submitted,

HARDING LAW OFFICES

/s/ Joseph R. Casey
Joseph R. Casey, Esq. (Iowa AT0014276)
1217 Army Post Road
Des Moines, Iowa 50315-5596
Telephone: (515) 287-1454
Facsimile: (515) 287-1442
joe@iowalegal.com
(*pro hac vice* pending)
Lead attorney to be noticed

KRALOVEC CONBOY

Joseph M. Conboy, (Illinois 6323756)
53 West Jackson Boulevard, Suite 1150
Chicago, IL 60604
Telephone: (312) 726-9000
Facsimile: (312) 726-9000
joe@kralovecconboy.com

ATTORNEYS FOR PLAINTIFF

VERIFICATION

I, Gerald Knoll, hereby state under oath that I have read the foregoing Complaint for *in personam* and *in rem* actions and know the contents thereof. The matters and things stated therein are true to the best of my knowledge, except those matters therein stated upon information and belief, and as to those matters, I believe them to be true.

I declare under penalty of perjury that the foregoing is true and correct.

DATED 25 JUNE 2024

Gerald Knoll